10/566504 Attorney's Docket No. 1032326-000330 14/20 Resultation 31 JAN 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re P	atent Application of	
Karine	VILLEGAS et al.	Group Art Únit:
Applic	ation No.:) Examiner:
Filed:	January 31, 2006	Confirmation No.:
For:	A METHOD OF SECURELY IMPLEMENTING A CRYPTOGRAPHY ALGORITHM OF THE RSA TYPE, AND A CORRESPONDING COMPONENT (As Amended)))))

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date <u>January 31, 2006</u>

James A LaBarre

Registration No. 28,632

P.O. Box 1404 Alexandria, Virginia 22313-1404 (703) 836-6620

IAP20 Res'0 FOT/FTO 31 JAN 2006

	ותו בט ווניט ש					
Substitute for form 1449A/PTO & 1449B/PTO	Complete if Known					
FIRST	Application Number	AU/56 504				
INFORMATION DISCLOSURE	Filing Date	January 31, 2006				
STATEMENT BY APPLICANT	First Named Inventor	Karine VILLEGAS et al.				
(use as many sheets as necessary)	Examiner Name					
Sheet 1 of 1	Attorney Docket Number	1032326-000330				

U.S. PATENT DOCUMENTS						
Examiner Initials	Document Number	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Issue/Publication Dat (MM-DD-YYYY)		

FOREIGN PATENT DOCUMENTS											
					STATUS						
Examiner Initials	Document Number	Kind Code (if known)	Country	Date of Publication (MM-DD-YYYY)	Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec
	*2 830 146	W	France	03-28-03			J 77/1	Х	V = 1		X
								<u> </u>			
			1				1		1		

NON-PATENT LITERATURE DOCUMENTS					
Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.				
	*C. AUMULLER et al., "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures",				
	Cryptographic Hardware and Embedded Systems, International Workshop, 08-13-2002, pages 260-275.				

*Copy Attached

Examiner	Date	
Signature	Considered	
	1 00.100.00	

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

Form Letters1